Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~In a computer network a method for detecting ARP spoofing, including~~ A method for detecting ARP spoofing in a computer network, the method comprising:

~~receiving an ARP reply on a port of a network device;~~

~~generating a data packet, wherein the data packet includes information from the ARP reply, and an identification of the port on which the ARP reply was received;~~

receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and

~~storing information contained in the data packet in a database of an ARP collector; and~~

analyzing ~~the information~~ at least one association in [[the]] a database accessible to the ARP collector to determine when ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.

2. (Currently Amended) The method of claim 1, wherein ~~the generating the data packet, which includes information from the ARP reply, includes encrypting the data packet~~ the data packet is encrypted by the first device.

3. (Canceled)

4. (Currently Amended) The method of claim 1, wherein ~~the information~~

~~stored in the database includes a MAC address of a device which generated an ARP reply, and an IP address given as a source IP address in the ARP reply, and~~ the at least one association includes a time at which [[the]] an associated ARP reply was received on [[the]] a port.

5. (Currently Amended) The method of claim [[1]] 4, wherein ~~the information stored in the database includes a MAC address of a device which generated the ARP reply, and an IP address given as a source IP address in the ARP reply, and a time at which the ARP reply was received on the port, and~~ the at least one association further includes an identification of the port ~~on which the ARP reply was received~~.

6. (Currently Amended) The method of claim 1, wherein when it is determined that there is a spoofed ARP reply, blocking [[the]] a port on which the spoofed ARP reply was received.

7. (Original) The method of claim 1, wherein when it is determined that there is a spoofed ARP reply, filtering a MAC address which generated the spoofed ARP reply at a port at which the spoofed ARP reply was received.

8. (Original) The method of claim 1 further comprising:

transmitting the data packet to the ARP collector; and

generating an alert when an ARP spoofing condition occurs.

9. (Currently Amended) In an ARP collector a method for detecting ARP spoofing, the method comprising:

receiving [[ATP]] ARP Tunnel Protocol (ATP) packets from a first subnet of a computer network;

receiving ATP packets from a second subnet of the computer network;

storing information from the ATP packets from the first subnet in a database of the ARP collector;

storing information from the ATP packets from the second subnet in the database of the ARP collector; and

analyzing the received ATP packets and information in ARP collector database to determine when a spoofed ARP reply has been received on a port of the computer network.

10. (Original) The method of claim 9, further comprising:

blocking a port of the computer network which received a spoofed ARP reply.

11. (Original) The method of claim 9, further comprising:

identifying a MAC address as a source for a spoofed ARP reply; and

filtering the identified MAC address at a port of the computer network which received the spoofed ARP reply.

12. (Original) The method of claim 9, wherein the ATP packets from the first subnet, and the ATP packets from the second subnet include ARP reply information received on ports of network devices in the respective subnets.

13. (Original) The method of claim 9, wherein the ATP packets from the first subnet, and the ATP packets from the second subnet include ARP reply information received on ports of network devices in the respective subnets, and information in the ATP packets includes information identifying a port on which a particular ARP reply was received.

14. (Original) The method of claim 9, wherein the storing information from the ATP packets from the first subnet, and the storing information from the ATP packets from the second subnet, includes:

storing ARP reply information indicating a MAC address which is identified as a source of an ARP reply,

storing ARP reply information indicating an IP address which is identified as a source of an ARP reply; and

storing information indicating a port on which an ARP reply was received.

15. (Currently Amended) A device for storing and analyzing ARP information to detect ARP spoofing, the device including:

an interface for receiving [[ATP]] ARP Tunnel Protocol (ATP) packets, wherein the ATP packets include ARP reply information, including information identifying a port on a network device where an ARP reply was received;

a processor coupled to the interface, and programmed to analyze a first received ATP packet, and to identify a first MAC address which is identified as a source MAC address for a first ARP reply, and to identify a first IP address which is identified as a source IP address for the first ARP reply, and to identify a first port on which the first ARP reply was received;

a database coupled to the processor, and which stores information from the ATP packets, wherein for the first ATP packet received at the interface, the database stores the first MAC address, the first IP address, and the port on which the first ARP reply was received; and

wherein the processor is further operable to analyze information in the database and information in a received ATP packet to identify when a spoofed ARP reply has been transmitted by a host, the analyzing being based upon a time associated with at least one entry stored in the database, the at least one entry including a MAC address that is identical to a MAC address included in the received ATP packet.

16. (Original) The device of claim 15, further including a garbage collection timer module which determines when ARP reply information is stale and should be cleared from the database.

17. (Original) The device of claim 15, wherein processor is further operable to generate an alert when a spoofed ARP reply has been detected.

18. (Original) The device of claim 15, wherein the processor is further operable, to identify a port on which a spoofed ARP reply has been received and to generate a signal which causes the port to be blocked in response to identifying the port on which the spoofed ARP reply has been received.

19. (Original) The device of claim 15, wherein the processor is further operable to identify a port on which a first spoofed ARP reply has been received and to identify a

MAC address of an attacking host which generated the spoofed ARP reply, and in response to identifying the port, and the MAC address of the attacking host, the processor generates a signal which indicates that the MAC address should be MAC filtered at the port.

20. (New) A method for detecting ARP spoofing in a computer network, the method comprising:

receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and

analyzing at least two associations in a database accessible to the ARP collector to determine when ARP spoofing occurs, wherein each of the at least two associations include a MAC address that is identical to the MAC address included in the data packet.

21. (New) The method of claim 1, wherein the MAC address and the IP address included in the data packet are stored as part of a first association in the database, wherein the first association includes a first time, and wherein analyzing at least one association in the database comprises:

identifying a second association in the database, wherein the second association includes a MAC address that is identical to the MAC address of the first association, an IP address that is identical to the IP address of the first association, and a second time;

identifying a third association in the database, wherein the third association includes a MAC address that is identical to the MAC address of the first association, an IP address that is different from the IP address of the first association, and a third time subsequent to the second time; and

determining when ARP spoofing occurs based on whether the first, second, and third times fall within a predefined time interval.